UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,812	11/29/2005	Christophe Justin Evrard	550-619	4576

23117 7590 11/12/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
VICARY, KEITH E	

ART UNIT	PAPER NUMBER
2183	

MAIL DATE	DELIVERY MODE
11/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte CHRISTOPHE JUSTIN EVRARD and JULIE-ANNE FRANCOISE MARIE PRUVOST

Appeal 2009-005011[1]
Application 10/527,812
Technology Center 2100

Decided: November 12, 2009

Before JOSEPH L. DIXON, JEAN R. HOMERE, and JAMES R. HUGHES, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] Filed November 29, 2005. The real party in interest is ARM Ltd. An oral hearing was held in this appeal on November 4, 2009.

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) (2002) from the final rejection of claims 1 through 10. We have jurisdiction under 35 U.S.C. § 6(b) (2008).

We affirm.

Appellants' Invention

Appellants invented a method and system for masking a write activity within a data processing system to thereby prevent unauthorized users from detecting the power consumption signature associated therewith. (Spec. 1, ll. 4-6, ll. 30-33.) As shown in Figure 1, upon receiving a conditional-write data instruction, a processor core (4) determines whether the instruction will effect a change to the state of the processor core (4). Upon determining that the instruction result, when written, will not cause a change, the processor core processes the conditional instruction and subsequently stores the results thereof in a trash register (51) instead of a data processing register (12) to make it difficult for an attacker to measure the power consumption associated with the stored results. (Spec. 2, ll. 1-4; Spec. 7, l. 25- Spec. 8, l. 1.)

Illustrative Claim

Independent claim 1 further illustrates the invention. It reads as follows:

> 1. Apparatus for processing data, said apparatus comprising:
>
> a processor core operable to execute data processing instructions to generate result data values; and

> data processing registers holding data values defining state of said processor core to which said result data values are written; wherein
>
> at least one data processing instruction executed by said processor core is a conditional-write data processing instruction encoding condition codes specifying conditions under which said conditional-write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core; and further comprising
>
> a trash register to which a result data value will be written instead of a data processing register upon execution of said conditional-write data processing instruction when said condition codes within said conditional-write data processing instruction do not permit a write to effect a change in state of said processor core.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Kissell	6,625,737 B1	Sept. 23, 2003
Qiu	6,804,782 B1	Oct. 12, 2004

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

1. Claims 1, 2, 5 through 7, and 10 stand rejected as being anticipated by Qiu.

2. Claims 3, 4, 8, and 9 stand rejected as being unpatentable over the combination of Qiu and Kissell.

Appellants' Contentions

First, Appellants contend that Qiu does not teach writing data results in a trash register instead of a data processing register when the codes of a

conditional instruction do not permit a write to effect a change in a processor core, as recited in independent claim 1. (App. Br. 8-10, Reply Br. 5-7.) According to Appellants, Qiu discloses an algorithm that produces a significant increase in activity within the power signature to mask any changes that could occur as a result of a conditional write in a data processing operation. (App. Br. 8) Thus, while both Qiu and the claimed invention are directed to solutions to preventing the characteristics associated with a write to a data processing register, Qiu's masking is simply different from the writing the results in a trash register instead of a data processing register, as required by the claim. (App. Br. 7.)

Next, Appellants contend that Qiu's masking approach teaches away from the claimed invention since Qiu's algorithm carries out unnecessary mathematical operations, whereas the claimed invention requires executing a single instruction based on the detected condition therewith. (App. Br. 10-11.)

Examiner's Findings

The Examiner finds that Qiu's disclosure of storing in a pseudo register the result of an unnecessarily performed multiplication operation to prevent an unauthorized user from deciphering a secret decryption key teaches the limitation of storing a result data value in a trash register instead of a data processing register, as recited in claim 1. (Ans. 10-12.) Further, the Examiner finds that Qiu's disclosure of determining whether to store the result of a multiplication operation in a trash register is conditioned on whether the value of a private key bit is "0" or "1" teaches the limitation of storing the data value result in the trash register upon executing a conditional-write data processing instruction when associated condition

codes do not permit a write to change the state of a processor core, as recited in claim 1. (Ans. 12-17.)

II. ISSUE

Therefore, the threshold issue before us is whether Appellants have shown that the Examiner erred in finding that Qiu teaches storing a data value result in the trash register instead of a data processing register upon executing a conditional-write data processing instruction when condition codes associated therewith do not permit a write to effect a change in the state of a processor core, as recited in claim 1?

III. FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

Qiu

1. Qiu discloses a circuit for combating power and timing attacks against cryptographic operations. In particular, Qiu discloses performing superfluous operations and storing data as a way to disguise the amount of power usage as well as the amount of time required to perform a cryptographic operation. (Abstract.)

2. As shown in Figures 1 through 3, upon receiving an encrypted message, a cryptographic algorithm is applied thereon to disguise the power and time required to decrypt the message. In one embodiment, a processor performs an unnecessary multiplication operation (emulated multiplication) in order to mask one or more bits of a private cryptographic key. The result

of the emulated multiplication operation is subsequently stored in a dummy memory location or in a data processing register. (Col. 1, ll. 45-67.)

3. Qiu discloses that when the additional (unnecessary) processes are conditional processes that one would expect to occur as part of a cryptographic algorithm, an attacker is likely to be fooled to rely upon the value of bit of a private key associated with the multiplication. In other words, the value bit "1" indicates that the multiplication is likely to occur, whereas the bit value "0" indicates that the multiplication is not likely to occur. Thus, the attacker's attempt to decipher the private key value is likely to be foiled. (Col. 3, ll. 47-67.)

4. As shown in Figure 5, Qiu discloses if the value key bit is "1," the result of the emulated multiplication is stored in a data processing memory location (512). If, however, the value key bit is "0," a dummy register (516) is used to store the result of the emulated multiplication operation. (Col. 6, ll. 5-27.)

IV. PRINCIPLES OF LAW

Anticipation

In rejecting claims under 35 U.S.C. § 102, "[a] single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation." *Perricone v. Medicis Pharm. Corp.*, 432 F.3d 1368, 1375 (Fed. Cir. 2005) (citing *Minn. Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 1565 (Fed. Cir. 1992)).

> Anticipation of a patent claim requires a finding that the claim at issue 'reads on' a prior art reference. In other words, if granting patent protection on the disputed claim would allow

> the patentee to exclude the public from practicing the prior art, then that claim is anticipated, regardless of whether it also covers subject matter not in the prior art.

Atlas Powder Co. v. IRECO, Inc., 190 F.3d 1342, 1346 (Fed. Cir. 1999) (internal citations omitted).

V. CLAIM GROUPING

Appellants argue the patentability of claim 1 in conjunction with the rejection of claims 2, 5 through 7, and 10. Similarly, Appellants argue the patentability of claim 3 in conjunction with the rejection of claims 4, 8, and 9. In accordance with 37 C.F.R. § 41.37(c)(1)(vii), we will consider claims 2, 5 through 7 and 10 as standing and falling with representative claim 1. We will similarly consider claims 4, 8, and 9 as standing and falling with representative claim 3.

VI. ANALYSIS

Anticipation

Claims 1, 2, 5 through 7, and 10

Independent claim 1 requires, in relevant part, storing a data value result in the trash register instead of a data processing register upon executing a conditional-write data processing instruction when condition codes associated therewith do not permit a write to effect a change in the state of a processor core.

We first consider the scope and meaning of the expressions "*conditional write data processing instruction*" and "*condition codes*," which must be given the broadest reasonable interpretation consistent with

Appellants' disclosure, as explained in *In re Morris*, 127 F.3d 1048 (Fed. Cir. 1997):

> [T]he PTO applies to the verbiage of the proposed claims the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in the applicant's specification.

Id. at 1054. *See also In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989) (stating that "claims must be interpreted as broadly as their terms reasonably allow."). Appellants' Specification states the following:

> FIG. 2 schematically illustrates a conditional instruction 24. This *conditional instruction may be part of an instruction set* which includes only some conditional instructions or part of an instruction set, such as the ARM instruction set, which is substantially fully conditional. The *condition codes 26 encode a set of processor state conditions in which the associated instruction either will or will not be executed.* As an example, *the condition codes 26 can be arranged to specify that the instruction 24 will not execute if the condition codes currently set in the system indicate a zero result*, a carry has occurred, an overflow has occurred or the like. This type of instruction can be utilised to provide efficient program coding. The fixed/variable bit at least partially suppresses the conditional behaviour in that the instruction will execute irrespective of its condition codes, but may not write its result in a way that has an effect upon the processor state.

(Spec. 6, ll. 4-15.) (emphasis added.)

Our reviewing court further states, "the 'ordinary meaning' of a claim term is its meaning to the ordinary artisan after reading the entire patent." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005).

Upon reviewing Appellants' Specification, we find no explicit definition for the recited claim expressions. Further, we find no explicit definition for the claimed "instruction" in the Specification, either.[2] We therefore broadly but reasonably construe the recited expressions in accordance with their ordinary meaning. In particular, we construe a "conditional-write data processing instruction" as a command (which may be part of a set of commands) to write to memory upon the occurrence of a predetermined condition. Similarly, we construe "conditional codes" as computer codes that permit a command to be executed upon the occurrence of a predetermined condition. Consistent with these definitions, we broadly but reasonably construe the disputed claim limitation in this appeal as requiring generated data result values to be written in a trash register instead of a data processing register when a processor core executes a write command that will not change the state of the processor core.

As set forth in the Findings of Facts, Qiu discloses storing the result of an emulated multiplication operation in a dummy register as opposed to a data processing register if the key value bit of an encryption algorithm is a "0." (FF. 4.) We find that Qiu's disclosure of a dummy register teaches the claimed trash register. Further, we find Qiu's disclosure of storing the emulated multiplication result in the dummy register is conditioned upon the processor receiving a command to perform an unnecessary operation, which

---

[2] Appellants provided a Wikipedia definition of "instruction" as a single operation of a processor defined by an instruction set architecture. The instruction may be any representation of an element of an executable program. (*See* Attachment cited in Reply Br. 11); *Cf.* Microsoft Press Computer Dictionary, 215 (2nd ed. 1994) (defining instruction as an action statement in any computer language).

will not change the state of the processor. We therefore agree with the Examiner that Qiu's disclosure teaches the disputed limitations, as construed above. We further agree with the Examiner that Appellants' argument that Qiu's disclosure relates to simple power analysis (SPA) whereas the invention relates to differential power analysis (DPA) is irrelevant in the present case. (Ans. 11.) We find no basis in the language of the claims before us to substantiate the distinctions that Appellants are seeking to establish. Thus, these arguments are not commensurate with the scope of the claimed invention. We also agree with the Examiner that Qiu's disclosure of performing the emulated multiplication teaches executing one or more data processing instructions to determine whether to store the result in a dummy register or a data processing register. (Ans. 14-17.)

Last, Appellants' argument that Qiu teaches away from the claimed invention (App. Br. 10-12, Reply Br. 7-8) is misplaced because the Examiner has rejected the claims under 35 U.S.C. § 102. Our reviewing court has determined that "[t]eaching away is irrelevant to anticipation." *Seachange Int'l, Inc., v. C-Cor, Inc.*, 413 F.3d 1361, 1380 (Fed. Cir. 2005)(citation omitted).

It follows that Appellants have not shown that the Examiner erred in finding that Qiu anticipates claim 1.

Obviousness

Claims 3, 4, 8, and 9

Appellants argue that the combination of Qiu and Kissell does not teach the trash register, as recited independent claim 1. We already

addressed this argument in the preceding paragraph, and we found that Qiu's dummy register teaches that limitation.

Next, Appellants argue that there is insufficient rationale for combining the teachings of Qiu and Kissell's. (App. Br.15.) In response, the Examiner finds that Qiu discloses disabling writing to a dummy register after a certain amount of iterations to prevent a total disruption of the process. (Ans. 7.) The Examiner further finds that Kissell discloses using a control signal to disable a signal line. (Ans. 8.) Consequently, the Examiner concludes that Qiu and Kissell disclose known prior art elements that perform their ordinary functions to predictably result in a system that uses control signals to disable writing to a dummy register. (Ans. 18.) We agree with the Examiner's findings and conclusion. Therefore, we adopt such findings and conclusion. It follows that Appellants have not shown that the Examiner erred in concluding that the combination renders the combination of Qiu and Kissell renders claim 3 unpatentable.

VII. CONCLUSIONS OF LAW

1. Appellants have not established that the Examiner erred in rejecting claims 1, 2, 5 through 7, and 10 as being anticipated by Qieu under 35 U.S.C. § 102.

2. Appellants have not established that the Examiner erred in rejecting claims 3, 4, 8, and 9 as being unpatentable over the combination of Qieu and Kissell under 35 U.S.C. § 103.

VIII. DECISION

We affirm the Examiner's rejections of claims 1 through 10.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

erc

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203